NCE & TECHNOLOGY:

AN ANALYSIS OF COMPUTER SECURITY SAFEGUARDS FOR DETECTING AND PREVENTING INTENTIONAL COMPUTER MISUSE

NBS Special Publication 500-25
U.S. DEPARTMENT OF COMMERCE
National Bureau of Standards

0-25

NATIONAL BUREAU OF STANDARDS

The National Bureau of Standards[1] was established by an act of Congress March 3, 1901. The Bureau's overall goal is to strengthen and advance the Nation's science and technology and facilitate their effective application for public benefit. To this end, the Bureau conducts research and provides: (1) a basis for the Nation's physical measurement system, (2) scientific and technological services for industry and government, (3) a technical basis for equity in trade, and (4) technical services to promote public safety. The Bureau consists of the Institute for Basic Standards, the Institute for Materials Research, the Institute for Applied Technology, the Institute for Computer Sciences and Technology, the Office for Information Programs, and the Office of Experimental Technology Incentives Program.

THE INSTITUTE FOR BASIC STANDARDS provides the central basis within the United States of a complete and consistent system of physical measurement; coordinates that system with measurement systems of other nations; and furnishes essential services leading to accurate and uniform physical measurements throughout the Nation's scientific community, industry, and commerce. The Institute consists of the Office of Measurement Services, and the following center and divisions:

Applied Mathematics — Electricity — Mechanics — Heat — Optical Physics — Center for Radiation Research — Laboratory Astrophysics[2] — Cryogenics[2] — Electromagnetics[2] — Time and Frequency[2].

THE INSTITUTE FOR MATERIALS RESEARCH conducts materials research leading to improved methods of measurement, standards, and data on the properties of well-characterized materials needed by industry, commerce, educational institutions, and Government; provides advisory and research services to other Government agencies; and develops, produces, and distributes standard reference materials. The Institute consists of the Office of Standard Reference Materials, the Office of Air and Water Measurement, and the following divisions:

Analytical Chemistry — Polymers — Metallurgy — Inorganic Materials — Reactor Radiation — Physical Chemistry.

THE INSTITUTE FOR APPLIED TECHNOLOGY provides technical services developing and promoting the use of available technology; cooperates with public and private organizations in developing technological standards, codes, and test methods; and provides technical advice services, and information to Government agencies and the public. The Institute consists of the following divisions and centers:

Standards Application and Analysis — Electronic Technology — Center for Consumer Product Technology: Product Systems Analysis; Product Engineering — Center for Building Technology: Structures, Materials, and Safety; Building Environment; Technical Evaluation and Application — Center for Fire Research: Fire Science; Fire Safety Engineering.

THE INSTITUTE FOR COMPUTER SCIENCES AND TECHNOLOGY conducts research and provides technical services designed to aid Government agencies in improving cost effectiveness in the conduct of their programs through the selection, acquisition, and effective utilization of automatic data processing equipment; and serves as the principal focus wthin the executive branch for the development of Federal standards for automatic data processing equipment, techniques, and computer languages. The Institute consist of the following divisions:

Computer Services — Systems and Software — Computer Systems Engineering — Information Technology.

THE OFFICE OF EXPERIMENTAL TECHNOLOGY INCENTIVES PROGRAM seeks to affect public policy and process to facilitate technological change in the private sector by examining and experimenting with Government policies and practices in order to identify and remove Government-related barriers and to correct inherent market imperfections that impede the innovation process.

THE OFFICE FOR INFORMATION PROGRAMS promotes optimum dissemination and accessibility of scientific information generated within NBS; promotes the development of the National Standard Reference Data System and a system of information analysis centers dealing with the broader aspects of the National Measurement System; provides appropriate services to ensure that the NBS staff has optimum accessibility to the scientific information of the world. The Office consists of the following organizational units:

Office of Standard Reference Data — Office of Information Activities — Office of Technical Publications — Library — Office of International Standards — Office of International Relations.

---

[1] Headquarters and Laboratories at Gaithersburg, Maryland, unless otherwise noted; mailing address Washington, D.C. 20234.

[2] Located at Boulder, Colorado 80302.

COMPUTER SCIENCE & TECHNOLOGY:

An Analysis of Computer Security Safeguards for Detecting and Preventing Intentional Computer Misuse

Brian Ruder and J.D. Madden

Stanford Research Institute
Menlo Park, California 94025

Robert P. Blanc, Editor

Institute for Computer Sciences and Technology
National Bureau of Standards
Washington, D.C. 20234

U.S. DEPARTMENT OF COMMERCE, Juanita M. Kreps, Secretary

Dr. Sidney Harman, Under Secretary

Jordan J. Baruch, Assistant Secretary for Science and Technology

U.S. NATIONAL BUREAU OF STANDARDS, Ernest Ambler, Acting Director

Issued January 1978

Reports on Computer Science and Technology

The National Bureau of Standards has a special responsibility within the Federal Government for computer science and technology activities. The programs of the NBS Institute for Computer Sciences and Technology are designed to provide ADP standards, guidelines, and technical advisory services to improve the effectiveness of computer utilization in the Federal sector, and to perform appropriate research and development efforts as foundation for such activities and programs. This publication series will report these NBS efforts to the Federal computer community as well as to interested specialists in the academic and private sectors. Those wishing to receive notices of publications in this series should complete and return the form at the end of this publication.

National Bureau of Standards Special Publication 500-25
Nat. Bur. Stand. (U.S.), Spec. Publ. 500-25, 80 pages (Jan. 1978)
CODEN: XNBSAV

Library of Congress Cataloging in Publication Data

Ruder, Brian.

An analysis of computer safeguards for detecting and preventing intentional computer misuse.

(Computer science & technology) (NBS special publication; 500-25)
Supt. of Docs. no.: C13.10:500-25

1. Computer crimes. 2. Computers—Access control. 3. Electronic data processing departments—Security measures. I. Madden, J. D., joint author. II. Title. III. Series. IV. Series: United States. National Bureau of Standards. Special publication ; 500-25.
QCI00.U57 no. 500-25 [HV6773] 602'.Is [364.1'62] 77-25368

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 1978)

For sale by the Superintendent of Documents, U.S. Government Printing Office
Washington, D.C. 20402. Price $2.40—Stock No. 003-003-01871-6

PREFACE

The work reported here was performed at Stanford Research Institute (SRI) for the National Bureau of Standards (NBS). The objectives of the study are to:

(1) Develop a working definition of intentional computer misuse and a taxonomy to characterize the different types of intentional computer misuse.
(2) Develop a ranked list of specific detection mechanisms.
(3) Develop a ranked list of specific prevention mechanisms.

The detection and prevention mechanisms were to be developed as a result of analysis of computer misuse case files, most of which are maintained by Mr. Donn B. Parker of SRI.

Robert P. Blanc, Editor
Staff Assistant for Computer
Utilization Programs
Institute for Computer Sciences
and Technology

TABLE OF CONTENTS

ILLUSTRATIONS

TABLES

AN ANALYSIS OF COMPUTER SECURITY SAFEGUARDS FOR DETECTING AND PREVENTING INTENTIONAL COMPUTER MISUSE

Brian Ruder
J. D. Madden
Stanford Research Institute
Menlo Park, California 94025

ABSTRACT

Stanford Research Institute (SRI) has an extensive file of actual computer misuse cases. The National Bureau of Standards asked SRI to use these cases as a foundation to develop ranked lists of computer safeguards that would have prevented or detected the recorded intentional misuses.

This report provides a working definition of intentional computer misuse, a construction of a vulnerability taxonomy of intentional computer misuse, a list of 88 computer safeguards, and a model for classifying the safeguards. In addition, there are lists ranking prevention and detection safeguards, with an explanation of the method of approach used to arrive at the lists.

The report should provide the computer security specialist with sufficient information to start or enhance a computer safeguard program.

KEY WORDS

Computer security; computer misuse; computer safeguards; computer security model; computer crime; computer fraud; privacy.

I. INTRODUCTION

A primary objective of this report is to identify computer safeguards that would have been useful in detecting and preventing actual cases of computer misuse. Section VI contains safeguard rankings based on cases of past intentional computer misuse. These cases span the spectrum of computer misuse, but the number of cases that fall into each vulnerability category probably do not reflect any one specific computer environment. Generally speaking, the highest ranking safeguards should be best in most environments, but the ranking process is somewhat subjective due to the nature of the cases and degree of detail specified in the safeguard description. Therefore, the rankings should not be considered absolute. Computer specialists should consider all tools as they develop their computer protection plan. A set of tools and a description of their purpose and application is provided in Appendix B.

This report contains the results of six work efforts, each of which is briefly described below.

The first effort involved developing a taxonomy of computer vulnerability to intentional computer misuse. The computer vulnerability taxonomy forms the foundation for the definition of intentional computer misuse as well as the foundation for categorizing past cases of computer misuse. Section II of this report contains this taxonomy.

The second effort was to develop a working definition of intentional computer misuse. The persons known to be studying the area of computer misuse throughout the country were contacted to determine their current definitions relating to computer abuse or computer misuse. The resulting definition of intentional computer misuse and a discussion of how the definition was arrived at are addressed in Section III of this report.

The third effort was to review the case file of computer misuses and distribute cases into appropriate vulnerability categories. Each case was placed in only one vulnerability category even though three or four misuses may have been identified in the case writeup. Each case was placed in the category corresponding to the first misuse identified in the case writeup.

The fourth effort was to review case files to identify the prevention and detection safeguard mechanisms in each case that would have mitigated the misuses in that case. The safeguards from a previous NSF study[1] as well as those gathered from other relevant source material were used as a base and were supplemented by the authors' experiences and ideas.

---

[1] "Computer System Integrity Research Program," National Science Foundation Grant DCR74-23774.

The fifth effort was to develop a safeguard model that would provide a basis for describing, identifying, and distributing each safeguard. The most useful model appeared to be one based on organizational structure. Consequently, safeguards were classified into categories bearing the names of the organizational element responsible for initiation or implementation of the safeguard. This type of model allows users of this report to change the model to reflect the structure of their organization. In addition, it clearly points out that computer security is an organizational problem and not just a data processing or internal audit problem. Section IV of this report provides a description of the model.

The sixth effort involved ranking the safeguard mechanisms within a vulnerability category. An algorithm was developed in which all tools were scored as to their effectiveness against the cases in each of the vulnerability categories. Since many of the cases had little information, or lacked specific technical information to permit determining how effective some of the safeguards might be, there is a subjectivity to the ranking process that we believe reflects SRI technical expertise and provides the best ranking possible. However, the reader should be aware that the ranking is not absolute and reflects the applicability of the safeguards against past cases of misuse. Section VI of this report contains the rankings.

II. TAXONOMY OF VULNERABILITY TO INTENTIONAL MISUSE

Three types of computer resources to be protected are identified as follows:

- Intellectual property (data and programs)
- Physical property (equipment and supplies)
- Computer services and processes

With regard to intellectual property, misuses include unauthorized modification, destruction, and disclosure. With regard to physical property, misuses include unauthorized modification, destruction and theft. With regard to services and processes, the misuses include unauthorized use (theft) or denial of authorized use. Within the intellectual property domain, it is worthwhile to identify whether or not the misuse occurred internally or externally to the computer system. Internal includes activities from the time data or programs are entered at a terminal by reading or by using some other input device until the time they are output at a printer, display terminal or other output device. External activities include all data preparation and data handling prior to the time the data are entered at an input device and after the data are output at an output device.

The vulnerability taxonomy described has 17 separate categories. This is the minimum number of categories required to differentiate the different types of intentional misuses as far as this study is concerned. Figure 1 provides a schematic diagram of the vulnerability taxonomy as described above. Appendix A provides definitions of each category.

III. DEFINITION OF INTENTIONAL COMPUTER MISUSE

The concept of intentional computer misuse is used throughout the study. The definition of intentional computer misuse is a function of the vulnerability taxonomy described in Section II. Intentional computer misuse is defined as an intentional act directed at or committed with a computer system or its associated external data or program activities in which there is:

- Unauthorized modification, destruction, or disclosure of intellectual property (data or programs), or
- Unauthorized modification, destruction, or theft of physical property (equipment and supplies), or
- Unauthorized use or denial of a computer service or process.

This definition defines intentional computer misuse from a data processing point of view, consistent with the objectives of this report.

IV. SAFEGUARD MODEL

A safeguard model provides a means of describing, identifying, and distributing safeguards. It was decided that the most useful model would reflect organizational structure. This model reflects responsibility for initiation or implementation of the safeguards. Developing a safeguard model that is structured around the organization points out to the security specialist and to management that computer security is the responsibility of many organizational elements. In addition, the model provides a convenient mechanism for assigning safeguards identified in this report. Figure 2 provides a schematic diagram that reflects the model we suggest. Insurance, personnel, and contracts are defined as staff activities, but could be placed at the same level as operations, data processing, security or audit. Following is a brief description of each element of the model:

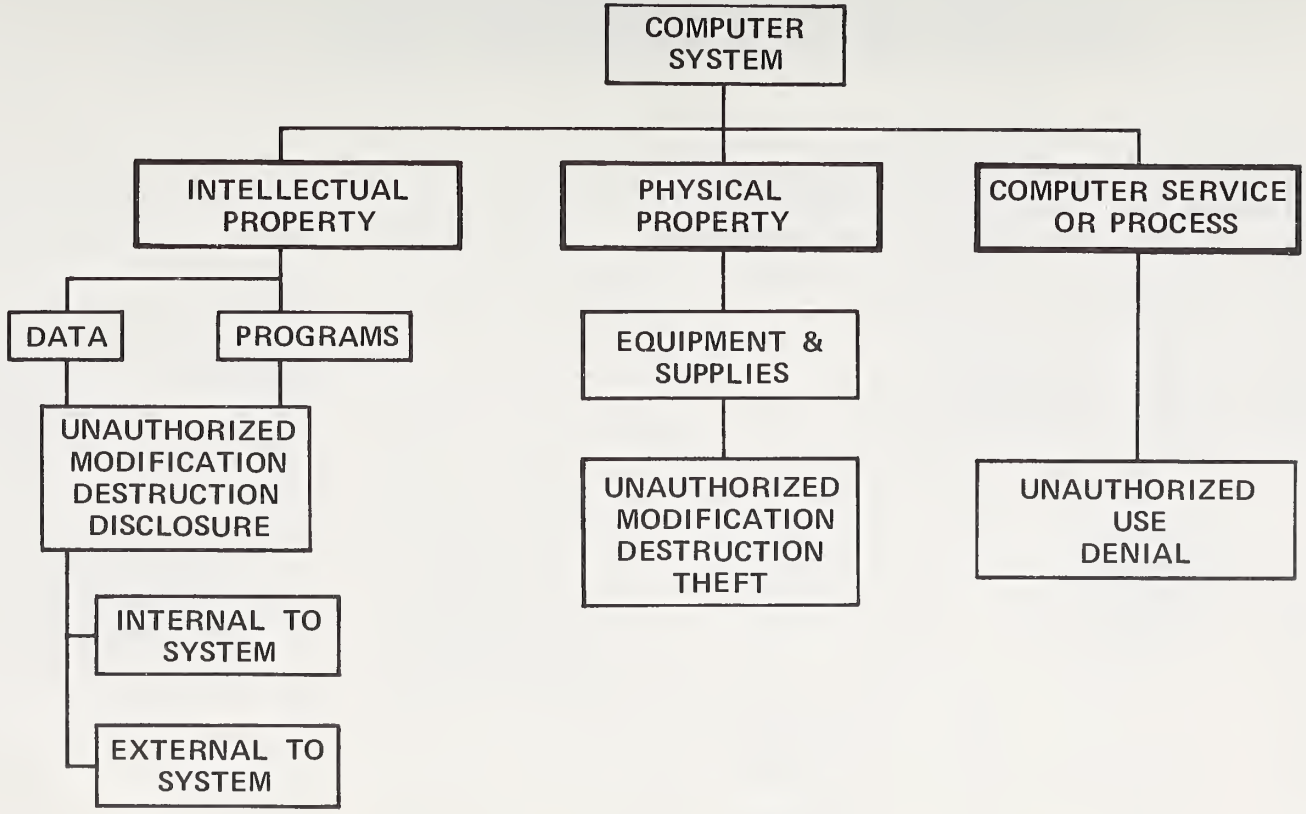

FIGURE 1 A TAXONOMY FOR VULNERABILITIES TO INTENTIONAL COMPUTER MISUSE

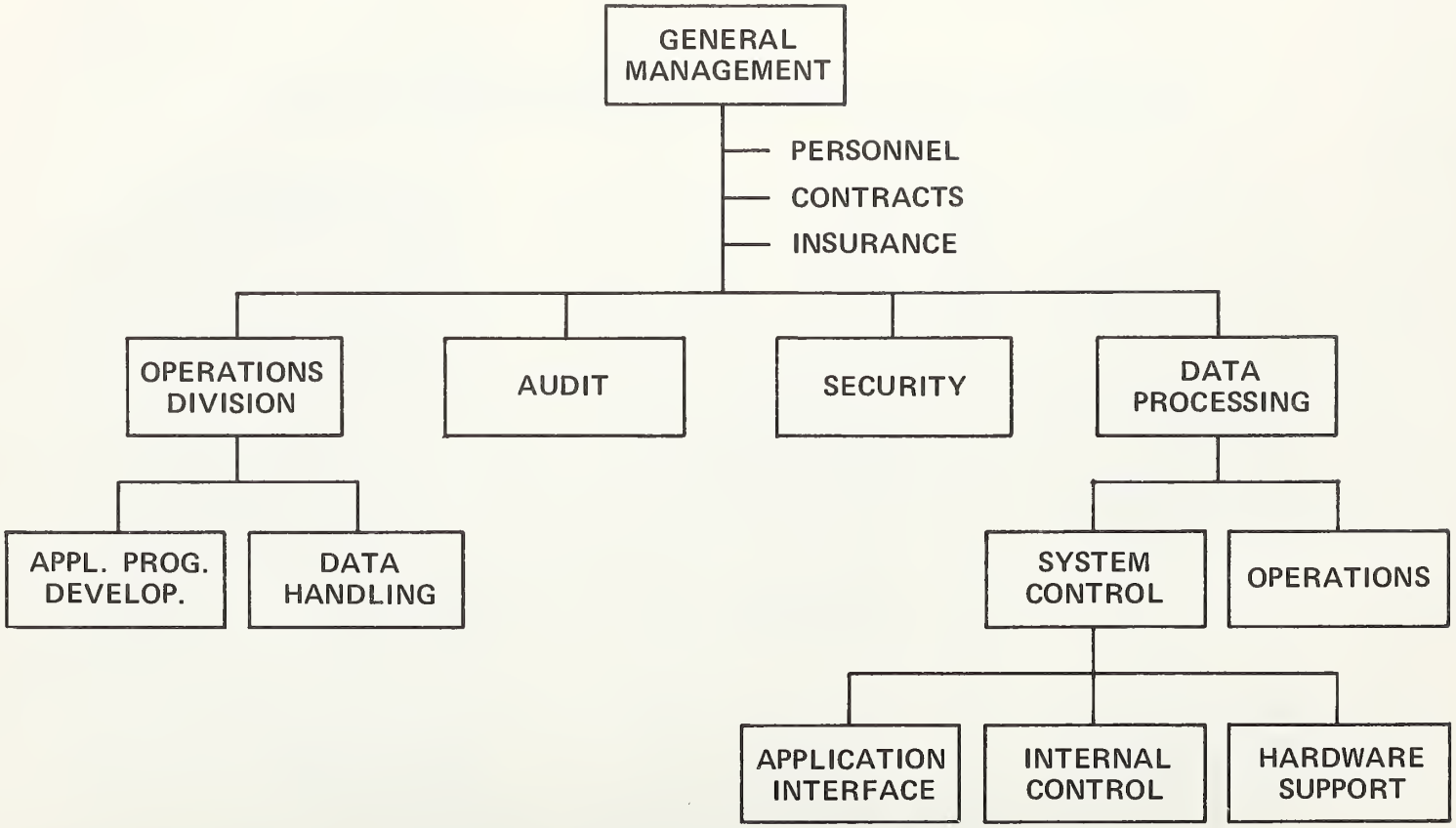

FIGURE 2 A MODEL FOR CATEGORIZING COMPUTER SAFEGUARDS ACCORDING TO RESPONSIBLE ORGANIZATIONAL UNIT

- General Management--This element includes those persons or functions whose primary responsibility is the management and administration of the agency. This element is responsible for establishing policy and ensuring that adequate financial and line management support is provided to carry out the agency charter.

- Personnel--This subelement is responsible for maintaining personal information on employees required by the agency as well as providing the official guidelines describing the policy of the agency regarding hiring and firing criteria.

- Contracts--This subelement is responsible for ensuring that all contracts, including those involving software and hardware, are well specified to minimize the potential for loss resulting from improper performance.

- Insurance--This subelement is responsible for ensuring that the facilities, including software and hardware, are adequately insured.

- Operations Division--Most Government agencies will have more than one operations division, but conceptually they are all similar from a data processing point of view. Consequently the model provides for only one operations division. An operations division is an organizational unit responsible for one general agency function such as logistics. Each operations division has many departments, but only two, application program development and data handling, are germane to the model.

- Application Program Development--For this report, all application program development and support are placed outside of data processing, even though many agencies provide application support within data processing. This placement was chosen for convenience to separate application program safeguards from system program safeguards. Application program development includes all facets of information collection and analysis, programming, and testing required to develop computer-based systems such as payroll, accounts payable and the like.

- Data Handling--This component includes all facets of data preparation, transport to and from input and output devices, and report distribution and storage.

- Audit--This element includes the internal audit and automatic data processing (ADP) audit function. (The audit safeguards in this report reflect primarily ADP auditing.) The responsibility of this element includes verification and evaluation of controls, standards, and data processing results.

- Security--This element is responsible for computer security, policy and coordination as well as traditional security items such as safes, locks, etc. Many agencies may have the computer security administration function located within the data processing function. Others believe it should be outside data processing to assure it can operate independently and objectively.

- Data Processing--This element includes the management and operation of all computer equipment, personnel and space to meet the agency's ADP requirements.

- System Control--This element is responsible for ensuring the integrity of the operating system and environment in which application programs execute. It has three components: Application Interface, Internal Control, and Hardware Support.

- Application Interface--This component is responsible for specifying application program standards and ensuring that all application systems are properly tested and documented. It is also responsible for program change control.

- Internal Control--This component is responsible for cataloging all internal controls available and ensuring that operational application system controls are in place and working. In addition, this component ensures that the operating system has adequate internal controls and is maintained properly.

- Hardware Support--This component is responsible for ensuring that hardware maintenance is performed in a reliable and valid manner. In addition, this component

is responsible for the acquisition and maintenance of any hardware required to support security safeguards.

- Operations--This element is responsible for the day-to-day operation of all computer equipment. It also is responsible for media backup, transport, and storage.

V. COMPUTER SECURITY PROGRAM REQUIREMENTS

This report is oriented toward identifying prevention and detection safeguards that would have been effective against actual cases of intentional computer misuse. There is, however, a requirement that an organization have an overall computer security program within which the safeguards can function. The basis for a computer security program is management policy and support that clearly define a computer security charter and its scope. Following is a brief discussion of basic elements required to establish such a program that will allow the prevention and detection safeguards to be effectively implemented and used. It is important to note that the following is a description of only one of various possible organizational structures. Further guidance will be forthcoming from NBS in the area of computer security program requirements.

Computer Security Policy and Control - General management must ensure that the agency has a computer security policy coordination function. This function may be the responsiblity of one or more persons who act as a focus for computer security policy and coordination. This function should reside outside data processing, but those responsible should work very closely with data processing management. In the suggested safeguard model, the policy and coordination function would reside with security. Its primary responsibilities are to develop workable computer security standards and to coordinate the acquisition or implementation of computer security safeguards. In addition, this function works closely with the audit function to verify compliance to standards and adequacy of safeguards in place.

ADP Audit Function - It is important to have well-trained ADP auditors within the audit function. The ADP audit function is a relatively new function that works almost exclusively verifying the accuracy and completeness of computer-based information systems. General management must ensure that the ADP audit function has a clearly defined charter that includes responsibilities of ADP auditors in each of the following areas:

1. System Development - the ADP auditor monitors the development process and acts as an advisor to the user regarding internal controls that should be designed into the application system. These controls include run-to-run totals, logging, and usage reports. The ADP auditor does not participate in the actual design or implementation of the system.

2. Testing - the ADP auditor ensures the adequacy of test procedures and verifies the existence and adequacy of internal controls.

3. Operations - the ADP auditor performs operational audits to ensure compliance to standards generated by the system control function and the data processing function. These include standards on items such as media labeling, handling and storage.

4. Post-installation Review - the ADP auditor works with the user to determine the actual characteristics of the system and whether they meet the users requirements as intended.

5. Thru-the-Computer-Audit - the ADP auditors should use the computer to assist them in auditing information accuracy and completeness. In particular, the auditors should include audit of data stored internally to the computer system, i.e., the auditors should not audit "around the computer."

System Design Standards - General management should ensure that internal controls and other security mechanisms are included among the system design considerations. Standards or guidelines should be established to ensure that they are included.

Insurance - General management should require that the ADP insurance program is current and that a risk assessment is made to establish the completeness of items insured and the amounts for which they are insured.

Contracts - General management should ensure that the responsible personnel in the contracts office are properly trained in ADP technology and terminology and are aware of particular problems associated with contracting for computer programs, ADP equipment, supplies and services.

It is important that general management recognize the importance of its role in any successful computer security program. A study for

the Institute of Internal Auditors recently completed by SRI indicates that general management support for audit and control programs needs to be improved if the integrity of computer-based information systems is to be ensured.

Safeguard Implementation Strategy - An important point to consider in developing a safeguard program is how the safeguards should be applied, i.e., the strategy of safeguarding computer systems. Providing a complete strategy is beyond the scope of this report, but a few basic considerations are provided.

First, the case files indicated that the most misused systems include:

- Payroll
- Accounts payable and receivable
- Certificate generating (license, stocks, etc.)
- Social payment (welfare and other benefits)
- Operating system (vendor-supplied system that runs the computer)

These systems should be protected first.

Second, the safeguards provided are broad in their application. The security specialist must consider the safeguards in the context of the specific environment.

Third, the method for determining which safeguards are best for a particular environment requires the establishment of a formal risk assessment. Guidelines for Automatic Data Processing Physical Security and Risk Management (FIPS PUB 31) and Automatic Data Processing Risk Assessment (NBSIR 77-1228) both published by NBS are excellent documents to start the risk assessment process. The most important item to recognize in performing a risk assessment is that no two ADP environments are the same and thus each environment must be evaluated to determine the best strategy for protecting it.

VI. SAFEGUARD ANALYSIS AND RANKINGS

Safeguard Classification

For this report, a safeguard is classified as a detection mechanism if it operates after the occurence of the misuse, regardless of whether it operates within a few seconds or a number of days after the misuse. In a number of cases, the time period in which the safeguard operates is a function of how it is implemented and used within an organization.

For example, some of the logging safeguards could be implemented to trigger an action when a specific type of record is encountered or to allow review of the record at the end of some specified time period, possibly a day.

A total of 88 safeguards are described in this report. Of these 32 are detection safeguards and 56 are prevention safeguards. Of the 32 detection safeguards, 15 are within the responsibility of the Audit function. Most audit safeguards are for use by ADP auditors. The ADP Audit function is rapidly becoming one of the most important functions within organizations concerned with vulnerabilities of computer systems.

The Internal Control element within the data processing function has responsibility for 19 safeguards because of the definition assigned to that element. It was given responsibility for many of the password safeguards that could fall under the security function. The Internal Control element is one of the most important security control functions as is the Audit function.

The 88 safeguards are listed in Table 1. Their order of listing is based on the safeguard model, with General Management safeguards first and those from Operations in Data Processing last. Within each organizational element category, the detection safeguards appear before prevention safeguards. An attempt has been made to list the highest ranking safeguards first within a given category. A "D" entry in the table indicates that the associated safeguard has some capability for detecting misuses in that vulnerability category. Similarly, a "P" entry indicates that the safeguard has some capability to prevent misuses in the indicated vulnerability category. Appendix B contains formatted descriptions of each of the safeguards. Safeguards in Appendix B are listed in the same order as they appear in Table 1.

Safeguard Rankings

Table 2 provides a list of the top 25 ranked detection safeguards within vulnerability categories, and Table 3 provides a similar list for the top 31 ranked prevention safeguards. Only those safeguards that were ranked in the top five on the basis of effectiveness for one of the vulnerability categories were included. A "1" entry in Table 2 or 3 indicates that the associated safeguard was deemed to be the most effective safeguard against the specified vulnerability category. As an example, for the vulnerability category in Table 2, Internal Program Disclosure, the five most effective detection safeguards, listing the most effective one first are:

RANK	DETECTION SAFEGUARD
1	User Command Log
2	Sensitive File Access Log
3	Operator Console Log
4	Media Usage Log
5	Computer Resource Usage Audit

It should be pointed out that not all vulnerability categories in either Tables 2 or 3 contain five ranked safeguards (e.g., the Computer Equipment and Supplies/Modification category in Table 3). The reason for this is that some vulnerability categories have fewer than five safeguards deemed effective.

One caution is indicated in interpreting Tables 2 and 3. The safeguards are ranked only within a given vulnerability category and can be considered valid over a reasonable range of installations. As previously mentioned, rankings, to some degree, are dependent on environment. For Tables 2 and 3 comparisons between vulnerability categories are meaningless. Tables 4 and 5 provide lists of safeguards ranked across all vulnerability categories.

Table 4 presents the eight most effective detection safeguards, and Table 5 presents the eight most effective prevention safeguards. For example, Table 5 indicates that on a consensus basis, Application System Design Verification is the most effective prevention safeguard and Data Center Access Control is ranked fifth.

Great care must be exercised in interpreting Tables 4 and 5. They are based on assumptions of limited validity at best.

To arrive at a consensus, an assumption was made that all vulnerability categories are of equal importance. It is unlikely, however, that this assumption is completely true for any given installation, and for some it may have no validity.

Another assumption made was that all of the safeguards are of the same degree of generality. The very general safeguards tend to receive a higher consensus score than the specific safeguards even though it may not be possible to implement the general safeguards completely, and their implementation is likely to be more expensive. In Table 4, Operations Area Surveillance is the highest ranked safeguard. If a single general audit safeguard had been used instead of 15 more specific safeguards, almost certainly the single audit would have ranked first.

Table 1

CONSOLIDATED LIST OF SAFEGUARDS

Safeguard by Organizational Entity	Internal						External						Computer Equipment and Supplies			System Service	
	Data			Program			Data			Program							
	M	DE	DI	M	DE	DI	M	DE	DI	M	DE	DI	M	DE	T	T	DN
General Management																	
1. Adjustment/Correction Reporting	D			D													
2. Job Rotation				D													
3. Disaster Avoidance								P			P			P			
Personnel																	
1. Employee Termination Policy		P	P		P	P		P	P		P	P		P			P
Operations Division																	
1. Mailing List Check			D						D								
2. External Data Responsibility Separation							P										
Application Program Development																	
1. Personal Record Access Check	D						D										
2. Record Volume Control	P						P										
3. Terminal Log-Off	P	P	P	P	P	P										P	P
Data Handling																	
1. Input/Output Count Comparison		D	D		D	D											
2. Input/Output Data Control							P		P	P		P					
3. Input/Output Data Storage							P	P	P	P	P	P					
4. Input/Output Data Movement Control							P		P	P		P					
5. External Sensitive Area Access Control							P	P	P	P	P	P					
6. Input/Output Data Movement Security							P		P								
7. Address Change Control							P										
8. User Interface Data Control							P										
Audit																	
1. Audit by Extended Records	D						D										
2. Audit by Parallel Simulation				D						D							
3. Code Comparison Audit				D						D							
4. Selected Transaction Audit	D						D										
5. Data Handling Audit							D	D	D								
6. Selected Area Audit	D						D										
7. Audit with Test Data				D						D							
8. Computer Resource Usage Audit			D			D										D	
9. Crash Log Audit																	D
10. Audit by Computer-Aided Flowcharting				D						D							
11. Generalized Audit Software	D						D										
12. Snapshot Audit				D						D							
13. Audit from Terminal	D						D										
14. Library Usage Audit	D		D	D		D	D		D	D		D					
15. Late Processing Audit	D			D			D			D							
16. Application System Design Verification	P	P	P	P	P	P		P	P		P	P	P	P	P	P	P

Note: M = Modification; DE = Destruction; DI = Disclosure; T = Theft; and DN = Denial.

Table 1 (Continued)

Safeguard by Organizational Entity	Internal						External						Computer Equipment and Supplies			System Service	
	Data			Program			Data			Program							
	M	DE	DI	M	DE	DI	M	DE	DI	M	DE	DI	M	DE	T	T	DN
Security																	
1. Operations Area Surveillance							D	D	D	D	D	D	D	D	D		
2. Area Alarm System							D	D	D	D	D	D	D	D	D		
3. Data Center Access Control													P	P	P		P
4. Fire Detection and Extinguishment								P			P			P			P
5. Internal Tampering Alarms													P		P		
6. Metal Detector														P	P		
7. X-ray Surveillance									P			P			P		
8. Package Control									P			P			P		
9. Off-Site Storage																	P
Data Processing																	
1. Computer Inventory Control													D		D		
2. Bill Back System																D	
3. Password Protection System	P	P	P	P	P	P										P	P
4. Program Change Control Log				P						P							
5. Utility Control	P	P	P	P	P	P											P
System Control																	
Application Interface																	
1. Application System Test	P	P	P	P	P	P										P	P
2. Program Standards	P	P	P	P	P	P										P	P
3. Test Isolation Control	P		P														
4. Internal Standard Label Control	P		P	P		P											
5. Documentation Control																P	P
Internal Control																	
1. User Command Log	D	D	D	D	D	D										D	D
2. Data Transformation			D						D								
3. Sensitive File Access Log	D	D	D	D	D	D										D	D
4. Operator Console Log	D	D	D	D	D	D										D	D
5. IPL Check				D						D							
6. Improper Log-on Control	D	D	D	D	D	D										D	D
7. Non-password Terminal User Verification	P	P	P	P	P	P										P	P
8. Store and Fetch Protection	P	P	P	P	P	P										P	P
9. Least Privilege Principle	P		P	P		P											
10. Privileged Use Controls	P	P	P	P	P	P										P	P
11. Secondary Storage Passwords	P	P	P	P	P	P											
12. Device ID	P		P	P		P											
13. Off-hour Terminal Disconnect	P	P	P	P	P	P										P	P
14. Password Generation	P	P	P	P	P	P										P	P
15. Password Print Suppress	P	P	P	P	P	P										P	P
16. System Masquerade Control	P	P	P	P	P	P										P	P
17. Simultaneous Access Control	P																
18. Storage Purge			P			P											
19. Processing Time Control																P	P
Hardware Support																	
1. Hardware Monitor																D	
2. Remote Encryption Capability									P								

Note: M = Modification; DE = Destruction; DI = Disclosure; T = Theft; and DN = Denial.

Table 1 (Concluded)

Safeguard by Organizational Entity	Internal						External						Computer Equipment and Supplies			System Service	
	Data			Program			Data			Program							
	M	DE	DI	M	DE	DI	M	DE	DI	M	DE	DI	M	DE	T	T	DN
Hardware Support (continued)																	
3. Encryption for Transport									P								
4. Communication Encryption			P														
5. Alternate Communication Paths																	P
Operations																	
1. Media Usage Log	D	D	D	D	D	D										D	
2. Input/Output Data Control							P		P	P		P					
3. Input/Output Data Storage							P	P	P	P	P	P					
4. Tape/Disk Movement Control									P			P					
5. External Sensitive Area Access Control							P	P	P	P	P	P					
6. Sensitive Operator Input Control	P		P	P		P											
7. File Backup Standard																	P
8. Card Password Protection	P	P	P	P	P	P										P	P
9. Sensitive Forms Control															P		
10. Expiration Date Control	P			P													P
11. Console Configuration Control	P	P	P	P	P	P										P	P
12. Configuration Control	P		P	P		P											

Note: M = Modification
DE = Destruction
DI = Disclosure
T = Theft
DN = Denial.

Table 2

RANKED DETECTION SAFEGUARDS

	Ranking																	
	Internal						External						Computer Equipment and Supplies			System Service	
	Data			Program			Data			Program							
	M	DE	DI	M	DE	DI	M	DE	DI	M	DE	DI	M	DE	T	T	DN
General Management																	
1. Adjustment/Correction Reporting	3						5										
Operations Division																	
1. Mailing List Check			2						2								
Audit																	
1. Audit by Extended Records	1						4										
2. Audit by Parellel Simulation				4						1							
3. Code Comparison Audit				1						4							
4. Selected Transaction Audit	2						1										
5. Data Handling Audit							2	2	3								
6. Selected Area Audit							3										
7. Audit with Test Data										2							
8. Computer Resource Usage Audit						5										2	
9. Crash Log Audit																	2
10. Audit by Computer-Aided Flowcharting				3						5							
11. Generalized Audit Software	4																
12. Snapshot Audit				5													
Security																	
1. Operations Area Surveillance								1	4		1	1	1	1	2		
2. Area Alarm System													2	2	3		
Data Processing																	
1. Computer Inventory Control													3		1		
2. Bill Back System																1	
Internal Control																	
1. User Command Log		1	3	2	1	1										3	1
2. Data Transformation			1						1								
3. Sensitive File Access Log	5	2	4		2	2										5	3
4. Operator Console Log		3	5		3	3										4	4
5. IPL Check										3							
6. Improper Log-on Control		5			5												5
Operations																	
1. Media Usage Log		4			4	4											

Note: M = Modification
DE = Destruction
DI = Disclosure
T = Theft
DN = Denial.

1 = most effective
.
.
.
5 = least effective

Table 3

RANKED PREVENTION SAFEGUARDS

	Ranking																
	Internal						External						Computer Equipment and Supplies			System Service	
	Data			Program			Data			Program							
	M	DE	DI	M	DE	DI	M	DE	DI	M	DE	DI	M	DE	T	T	DN
General Management																	
2. Disaster Avoidance														5			
Personnel																	
1. Employee Termination Policy		1			1			2			2			3			
Operations Division																	
2. External Data Responsibility Separation							1										
Application Program Development																	
2. Record Volume Control							2										
Data Handling																	
2. Input/Output Data Control							3		1	4		1					
3. Input/Output Data Storage							5	3	5	1	3	5					
4. Input/Output Data Movement Control									4			4					
5. External Sensitive Area Access Control								5									
Audit																	
16. Application System Design Verification	1	2	1		2	1											1
Security																	
3. Data Center Access Control													1	1	1		
4. Fire Detection and Extinguishment								1			1			2			
5. Internal Tampering Alarms													2		2		
6. Metal Detector														4	4		
7 X-ray Surveillance															3		
8. Package Control															5		
Data Processing																	
3. Password Protection System		4	3	1	4	3										1	
4. Program Change Control Log				4													
5. Utility Control																	5
System Control																	
Application Interface																	
1. Application System Test	2	3	2	3	3	2											2
Internal Control																	
7. Non-Password Terminal User Verification				2												2	
8. Store and Fetch Protection	5	5		5	5												3
9. Least Privilege Principle	3		5			5											
10. Privileged Use Controls																3	4
11. Secondary Storage Passwords			4			4											
12. Device ID	4																
13. Off-hour Terminal Disconnect																5	
Operations																	
2. Input/Output Data Control							4		2	5		2					
3. Input/Output Data Storage								4		2	4						
4. Tape/Disk Movement Control									3			3					
5. External Sensitive Area Access Control										3	5						
6. Sensitive Operator Input Control																4	

Note: M = Modification T = Theft
DE = Destruction DN = Denial
DI = Disclosure

Table 4

CONSENSUS RANKING: DETECTION SAFEGUARDS

	Ranking
Security	
1. Operations Area Surveillance	1
Internal Control	
1. User Command Log	2
3. Sensitive File Access Log	3
2. Data Transformation	4
Security	
2. Area Alarm System	5
Audit	
5. Data Handling Audit	6
Internal Control	
4. Operator Console Log	7
Audit	
4. Selected Transaction Audit	8

Table 5

CONSENSUS RANKING: PREVENTION SAFEGUARDS

	Ranking
Audit	
16. Application System Design Verification	1
Application Interface	
1. Application System Test	2
Personnel	
1. Employee Termination Policy	3
Data Processing	
3. Password Protection System	4
Security	
3. Data Center Access Control	5
4. Fire Detection and Extinguishment	6
Data Handling	
2. Input/Output Data Control	7
3. Input/Output Data Storage	8

VII. SUMMARY AND CONCLUSIONS

This report provides a foundation for the development of a computer safeguard program directed toward the detection and prevention of intentional computer misuse. The definition of intentional computer misuse and the construction of an associated vulnerability taxonomy are believed to be comprehensive and complete. The safeguards described in the report were developed as a result of analysis of actual cases of computer misuse on record at SRI and other research organizations. The safeguards are ranked within each vulnerability category and across all categories, but the rankings are not absolute.

Three final considerations are noteworthy. First, to develop a safeguard program, it is necessary to know what safeguards are required and who is responsible for their initiation or implementation. In this report an organizational model for assigning responsibility is presented. Whereas the model provides a good classification scheme for this report, it requires additional work to show the interrelationships between general management, line management, and staff employees. The model indicates that all elements of an agency or organization have some responsibility for computer security, but it does not address the responsibilities of individuals.

Secondly, it would be useful to have a comprehensive format to describe safeguards. In a review of an actual case of misuse, a specific safeguard that would prevent or detect that misuse can be conceived. When a new but similar case is reviewed, the same safeguard with slight modification is required. After twenty to thirty such reviews, one either has twenty specific but very similar safeguards or the tool description becomes somewhat general. In describing the safeguards, this report attempts to provide sufficient detail for the security specialist. Nonetheless, a comprehensive safeguard description format would allow many different organizations to report safeguards in a standard format.

Thirdly, it is outside the scope of this report to describe different safeguard implementation strategies. A formal risk assessment must be performed as a necessary step in determining the safeguard implementation strategy for any particular environment.

VULNERABILITY CATEGORY DEFINITIONS

Following are definitions of the seventeen vulnerability categories that make up the vulnerability taxonomy. Modification has been defined to include selective destruction in which the intent of the destruction is personal gain--e.g., destroying a record of a personal bill. Destruction has been restricted to include malicious acts in which the primary intent was to cause damage--e.g., throwing disk packs out the window.

1. Unauthorized Modification of Data Internal to the Computer System (DMI)

   Vulnerabilities include unauthorized modification of computer data residing within the computer system proper. Covered are insertion of new data and modification or deletion of existing data by using an application system, system programs, or system facilities.

2. Unauthorized Destruction of Data Internal to the Computer System (DDeI)

   Vulnerabilities include unauthorized destruction of computer data residing within the computer system proper. Entailed is the intentional arbitrary destruction of existing data by using an application system, system programs, or system facilities.

3. Unauthorized Disclosure of Data Stored Internal to the Computer System (DDiI)

   Vulnerabilities include unauthorized disclosure of computer data residing within the computer system proper. Entailed is the disclosure to unauthorized persons of existing data obtained by using an application system, system programs, or system facilities.

4. Unauthorized Modification of Programs Internal to the Computer System (PMI)

   Vulnerabilities include unauthorized modification of programs residing within the computer system proper. Covered are insertion of new program modules and modification or deletion of existing programs by using an application system, system programs, or system facilities.

5. Unauthorized Destruction of Programs Internal to the Computer System (PDeI)

   Vulnerabilities include unauthorized destruction of programs residing within the computer system proper. Entailed is the intentional arbitrary destruction of existing programs by using an application system, system programs, or system facilities.

6. Unauthorized Disclosure of Programs Stored Internal to the Computer System (PDiI)

   Vulnerabilities include unauthorized disclosure of programs residing within the computer system proper. Entailed is the disclosure to unauthorized persons of existing programs obtained by using an application system, system programs, or system facilities.

7. Unauthorized Modification of Data External to the Computer System (DME)

   Vulnerabilities include unauthorized physical modification of computer data residing outside the computer system proper. Examples of misuse that might be committed during data origination, data preparation, or input handling are insertion of new data and modification or deletion of existing data.

8. Unauthorized Destruction of Data External to the Computer System (DDeE)

   Vulnerabilities include unauthorized physical destruction of computer data residing outside the computer system proper. Entailed is the intentional arbitrary destruction of data destined either as input to the system or output from the system.

9. Unauthorized Disclosure of Data Stored External to the Computer System (DDiE)

   Vulnerabilities include unauthorized disclosure of computer data residing outside the computer system proper. Entailed is the disclosure to unauthorized persons of data destined either as input to the system or output from the system.

10. Unauthorized Modification of Programs External to the Computer System (PME)

Vulnerabilities include unauthorized modification of programs residing outside the computer system proper. Covered are insertion of new program modules and modification or deletion of existing programs stored on cards, tapes, or disks, possibly by using outside computer facilities.

11. Unauthorized Destruction of Programs External to the Computer System (PDeE)

Vulnerabilities include unauthorized destruction of programs residing outside the computer system proper. Entailed is the intentional arbitrary destruction of existing programs stored on cards, tapes, or disks, possibly by using outside computer facilities.

12. Unauthorized Disclosure of Programs Stored External to the Computer System (PDiE)

Vulnerabilities include unauthorized disclosure of programs residing outside the computer system proper. Entailed is the disclosure to unauthorized persons of existing programs stored on listings, cards, tapes, disks, or other storage media, possibly by using outside computer facilities.

13. Unauthorized Modification of Computer Equipment or Supplies (CE&SM)

Vulnerabilities include unauthorized physical modification of computer system equipment or supplies. Covered are insertion of a new element, substitution of one element for another, and modification or deletion of an existing element with intent to benefit or for malicious reasons.

14. Unauthorized Destruction of Computer Equipment or Supplies (CE&SDe)

Vulnerabilities include unauthorized physical destruction of computer system equipment and supplies. Entailed is intentional arbitrary destruction.

15. Theft of Computer Equipment or Supplies (CE&ST)

Vulnerabilities include theft of computer system equipment or supplies with intent to benefit or for malicious reasons.

16. Unauthorized Use of Computer System Services (SST)

Vulnerabilities include the unauthorized use of any computer system services or resources.

17. Denial of Computer System Services (SSD)

Vulnerabilities include the denial of computer system services to authorized users. Entailed is the intentional denial of system services.

Appendix B

FORMATTED SAFEGUARD DESCRIPTIONS

Each of the 88 safeguards is described in this appendix. They are listed in the same order as they are presented in Table 1. The CATEGORY descriptor identifies the organizational element responsible for the safeguard. The COMMENTS descriptor indicates whether the safeguard must be designed into the system or environment or whether retrofit is possible. In some instances, the COMMENTS section contains additional information believed to be useful in understanding special characteristics of the safeguard.

For convenience the last page of this appendix contains an alphabetized listing of all vulnerability category abbreviations with associated meanings.

NAME: Adjustment/Correction Reporting

CATEGORY: General Management 1

DESCRIPTION: Policy, procedures, and software to provide reports of adjustment/correction transactions covering the sphere of influence for each manager. For example, any modification, updates, deletions, or other changes to the payroll master file should be reported regularly to the manager of payroll systems for his information and action.

PURPOSE: To detect unauthorized modification of data.

APPLICABLE VULNERABILITY CATEGORIES: DMI, DME

COMMENTS: Retrofit

NAME: Job Rotation

CATEGORY: General Management 2

DESCRIPTION: Policy and procedures to periodically rotate those positions that have a great deal of authority among individuals in the data handling process. For example, the position responsible for address changes should be assumed by new persons periodically and without notice. The new person's first responsibility would be to verify the integrity of the file.

PURPOSE: To detect unauthorized modification of data.

APPLICABLE VULNERABILITY CATEGORIES: DME

COMMENTS: Retrofit

NAME: Disaster Avoidance

CATEGORY: General Management 3

DESCRIPTION: Policy that facilities, both central and remote, are to be designed and constructed (or modified) so as to provide maximum protection against natural disasters and against persons intent on destroying physical or intellectual property. Documents, such as Guidelines for Automatic Data Processing Physical Security and Risk Management, FIPS PUB 31, can be used to assess the vulnerability to natural disasters.

PURPOSE: To prevent unauthorized destruction of data, programs, system equipment, or supplies.

APPLICABLE VULNERABILITY CATEGORIES: DDeE, PDeE, CE&SDe

COMMENTS: Although this safeguard is important even after facilities have been constructed and occupied, it is of greater value when planning new facilities.

NAME: Employee Termination Policy

CATEGORY: Personnel 1

DESCRIPTION: Policy and procedures to effect immediate restriction of terminated employee's access to sensitive material and areas. The intent of this safeguard is to ensure that disgruntled terminated employees are not in the position to destroy or disclose facilities or information.

PURPOSE: To prevent destruction (or denial) of data, programs, equipment, or services and unauthorized disclosure of data and programs.

APPLICABLE VULNERABILITY CATEGORIES: DDiI, PDeI, PDiI, DDeE, DDiE, DDeI, PDeE, PDiE, CS&EDe, SSD

COMMENTS: Retrofit; There were numerous cases in the file in which disgruntled employees destroyed data, programs, or equipment after their termination notice but before their actual departure.

NAME: Mailing List Check

CATEGORY: Operations Division 1

DESCRIPTION: Policy and procedures to insert dummy names with known addresses into mailing lists. Receipt of mail at these addresses will indicate that the mailing list is being misused. This will detect unauthorized disclosure of sensitive internal lists.

PURPOSE: To detect unauthorized disclosure and usage of sensitive internal use only mailing lists.

APPLICABLE VULNERABILITY CATEGORIES: DDiI, DDiE

COMMENTS: Retrofit

NAME: External Data Responsibility Separation

CATEGORY: Operations Division 2

DESCRIPTION: Policy and procedure to ensure that functions at critical points in the data-handling process are carried out by different individuals. For example, the same person should not handle address changes and establishment of new accounts.

PURPOSE: To prevent unauthorized modification of data.

APPLICABLE VULNERABILITY CATEGORIES: DME

COMMENTS: Retrofit

NAME: Personal Record Access Check

CATEGORY: Application Program Development 1
(Operations Division)

DESCRIPTION: Procedures and software to monitor and log access of users to their own records. For example, software can be added to the application program that maintains a list of authorized users with personal records in the file. Each time one of these persons accesses the file, a record is sent to the log and reviewed by appropriate personnel. For files such as payroll, the program will have to ascertain whether or not the person has access to his or her data; if so, additional programming may be required.

PURPOSE: To detect unauthorized modification of data.

APPLICABLE VULNERABILITY CATEGORIES: DMI, DME

COMMENTS: Retrofit

NAME: Record Volume Control

CATEGORY: Application Program Development 2
(Operations Division)

DESCRIPTION: Procedures and software to require specification and checking of I/O record volume by programs. For example, application systems should have control points where input/output record counts are reconciled before the next job step is initiated.

PURPOSE: To prevent unauthorized modification of data.

APPLICABLE VULNERABILITY CATEGORIES: DMI, DME

COMMENTS: Retrofit

NAME: Terminal Log-off

CATEGORY: Application Program Development 3 (Operations Division)

DESCRIPTION: Software to provide automatic log-off of a terminal that has been idle for a specified time interval. The length of time will vary with the type of system and terminal access controls in use.

PURPOSE: To prevent unauthorized modification, destruction, or disclosure of intellectual property or denial or theft of service or process.

APPLICABLE VULNERABILITY CATEGORIES: DMI, DDeI, DDiI, PMI, PDeI, PDiI, SST, SSD

COMMENTS: Retrofit

NAME: I/O Volume Count Comparison

CATEGORY: Data Handling 1 (Operations Division)

DESCRIPTION: Procedures and software to ensure that users compare I/O volume against predicted requirements. For example, the person responsible for making modifications to the payroll file should be required to predict the number of records to be changed and verify that exactly this number was changed.

PURPOSE: To detect unauthorized destruction, disclosure (or theft) of data or programs.

APPLICABLE VULNERABILITY CATEGORIES: DDeI, DDiI, PDeI, PDiI

COMMENTS: Retrofit

NAME: I/O Data Control

CATEGORY: Data Handling 2 (Operations Division)
Operations 2 (Data Processing)

DESCRIPTION: Procedures to ensure that specific control points exist for data movement throughout the user area. The intent is to provide for traceability and accountability.

PURPOSE: To prevent unauthorized modification or disclosure of data or programs.

APPLICABLE VULNERABILITY CATEGORIES: DME, DDiE, PME, PDiE

COMMENTS: Retrofit; The most numerous incidents of misuse identified are in the data-handling areas outside the computer system. Each organization has to develop specific control points that are meaningful within the context of its environment.

NAME: I/O Data Storage

CATEGORY: Data Handling 3 (Operations Division)
Operations 3 (Data Processing)

DESCRIPTION: Procedures and facilities to provide lockable storage for sensitive data, programs, and reports. This safeguard is not directed at government classified material.

PURPOSE: To prevent unauthorized modification, destruction, or disclosure of data or programs.

APPLICABLE VULNERABILITY CATEGORIES: DME, DDeE, DDiE, PME, PDeE, PDiE

COMMENTS: Retrofit; In a large number of cases, had safes or other lockable storage been used, not only would much of the data disclosure problem been solved, but much of the data and program destruction problem would have been reduced.

NAME: I/O Data Movement Control

CATEGORY: Data Handling 4 (Operations Division)

DESCRIPTION: Procedures to use transmittal slips to effect positive controls (such as traceability) over data being moved between user areas and the computer center.

PURPOSE: To prevent unauthorized modification or disclosure of data or programs.

APPLICABLE VULNERABILITY CATEGORIES: DME, DDiE, PME, PDiE

COMMENTS: Retrofit

NAME: External Sensitive Area Access Control

CATEGORY: Data Handling 5 (Operations Division)
Operations 5 (Data Processing)

DESCRIPTION: Procedures and facilities to deny or control unauthorized personnel access to sensitive user work areas. The intent of this safeguard is to ensure that a minimum number of people have access to user work areas where they might be able to change records that are in a format they understand.

PURPOSE: To prevent unauthorized modification, destruction or disclosure of data or programs.

APPLICABLE VULNERABILITY CATEGORIES: DME, DDeE, DDiE, PME, PDeE, PDiE

COMMENTS: Retrofit

NAME: I/O Data Movement Security

CATEGORY: Data Handling 6 (Operations Division)

DESCRIPTION: Procedures and facilities to provide lockable containers for moving data and output between user areas and the computer center or remote entry stations.

PURPOSE: To prevent unauthorized modification or disclosure of data.

APPLICABLE VULNERABILITY CATEGORIES: DME, DDiE

COMMENTS: Retrofit

NAME: Address Change Control

CATEGORY: Data Handling 7 (Operations Division)

DESCRIPTION: Procedures to provide special controls over receipt and validation of address change data. Of specific interest are addresses to which checks or other sensitive documents are sent. A large number of cases involved the establishment of ficticious companies and changing the accounts payable system to send checks to that company. Usually the system was not actually modified, but rather false entries were introduced by authorized users.

PURPOSE: To prevent unauthorized modification of data.

APPLICABLE VULNERABILITY CATEGORIES: DME

COMMENTS: Retrofit

NAME: User Interface Data Control

CATEGORY: Data Handling 8 (Operations Division)

DESCRIPTION: Procedures to provide for special controls, such as brief memoranda, over receipt and validation of data supplied directly by third parties, outside the normal procedures. The intent of this safeguard is to prevent persons such as programmers from calling the operator to change or fix programs in emergency situations without proper documentation.

PURPOSE: To prevent unauthorized modification of data.

APPLICABLE VULNERABILITY CATEGORIES: DME

COMMENTS: Retrofit

NAME: Audit by Extended Records

CATEGORY: Audit 1

DESCRIPTION: Procedures and software to enable application programs to append audit information to the transaction record, thus providing a complete audit trail contained as a part of the transaction. For example, a billing transaction might have recorded items such as:

- A reason code for credits or adjustments
- A code to indicate whether it was a back-ordered item
- A code to indicate whether pricing was special and who authorized it

PURPOSE: To detect unauthorized modification of data.

APPLICABLE VULNERABILITY CATEGORIES: DMI, DME

COMMENTS: Difficult to retrofit into existing application systems.

NAME: Audit by Parallel Simulation

CATEGORY: Audit 2

DESCRIPTION: Procedures and software to process production transactions with programs that simulate critical aspects of application system logic and to verify selected processing functions by comparing simulation results to production processing results. For example, a bank simulates savings interest calculations for all of its passbook savings customers. Since the simulation program verifies only the interest accrual calculations, it is much less complex than the passbook update application system.

PURPOSE: To detect unauthorized modification of programs.

APPLICABLE VULNERABILITY CATEGORIES: PMI, PME

COMMENTS: Retrofit

NAME: Code Comparison Audit

CATEGORY: Audit 3

DESCRIPTION: Procedures and software to compare two source programs, one of which is a control program, and identify differences. After this comparison, the auditor verifies that differences have been authorized by appropriate personnel and are properly documented.

PURPOSE: To detect unauthorized modification of programs.

APPLICABLE VULNERABILITY CATEGORIES: PMI, PME

COMMENTS: Retrofit

NAME: Selected Transaction Audit

CATEGORY: Audit 4

DESCRIPTION: Procedures and software to allow audit subroutines to execute with, but independent of, application systems to screen and select for later review any transactions of interest. The kinds of transactions to be selected are determined by a set of input parameters at the time the audit subroutines are exercised.

PURPOSE: To detect unauthorized modification of data.

APPLICABLE VULNERABILITY CATEGORIES: DMI, DME

COMMENTS: Difficult to retrofit into existing application systems; many of the misuses associated with financial systems would have been detected in the early stages had this safeguard been in use and used regularly.

NAME: Data Handling Audit

CATEGORY: Audit 5

DESCRIPTION: Procedures to conduct a periodic audit of the data preparation process. The audit verifies conformance to controls dictated by policies, standards, and procedures.

PURPOSE: To detect unauthorized modification, destruction, or disclosure of data or nonconformance to standards.

APPLICABLE VULNERABILITY CATEGORIES: DME, DDeE, DDiE

COMMENTS: Retrofit; Since the data handling area offers the most potential for misuse, it requires special audits of conformance to standard operating procedures.

NAME: Selected Area Audit

CATEGORY: Audit 6

DESCRIPTION: Procedures and software to collect and evaluate selected operating statistics to identify unexpected variations, such as a high level of uncollected receivables. Actual values collected are compared with predicted values.

PURPOSE: To detect unauthorized modification of data.

APPLICABLE VULNERABILITY CATEGORIES: DMI, DME

COMMENTS: Retrofit

NAME: Audit with Test Data

CATEGORY: Audit 7

DESCRIPTION: Procedures and software to execute application systems, such as payroll or accounts payable, using test data sets to verify accuracy of systems by comparing actual processing results with predetermined test results. This safeguard is used mostly with batch systems.

PURPOSE: To detect unauthorized modification of programs.

APPLICABLE VULNERABILITY CATEGORIES: PMI, PME

COMMENTS: Retrofit

NAME: Computer Resource Usage Audit

CATEGORY: Audit 8

DESCRIPTION: Procedures and software to select, extract, and analyze computer resource usage information and compare it against projected usage budget. Analysis is performed at the organization, organizational subdivision, and user levels. For example, a specific project may be budgeted for 2-3 hours of terminal usage during any week. If one week the project uses 7-10 hours, a check should be made to ensure that there is a valid reason for the extra usage.

PURPOSE: To detect unauthorized disclosure (or theft) of data, programs or services.

APPLICABLE VULNERABILITY CATEGORIES: DDiI, PDiI, SST

COMMENTS: Retrofit

NAME: Crash Log Audit

CATEGORY: Audit 9

DESCRIPTION: Procedures and software to collect and analyze system crash information for trends and evidence of intentional crashing. The intent is to ensure that a program exists for verifying that all system outages are explainable.

PURPOSE: To detect denial of system service.

APPLICABLE VULNERABILITY CATEGORIES: SSD

COMMENTS: Retrofit

NAME: Audit by Computer-Aided Flowcharting

CATEGORY: Audit 10

DESCRIPTION: Procedures and software to process application systems to automatically identify and present logic paths and control points. The flowcharts produced are then compared with those provided by the programmer to identify inconsistencies.

PURPOSE: To detect unauthorized modification of programs.

APPLICABLE VULNERABILITY CATEGORIES: PMI, PME

COMMENTS: Retrofit

NAME: Generalized Audit Software

CATEGORY: Audit 11

DESCRIPTION: Procedures and software to access, extract, manipulate, and present data and test results in a format appropriate to internal audit objectives. A number of generalized audit software packages are commercially available that offer various degrees of sophistication.

PURPOSE: To detect unauthorized modification of data.

APPLICABLE VULNERABILITY CATEGORIES: DMI, DME

COMMENTS: Retrofit

NAME: Snapshot Audit

CATEGORY: Audit 12

DESCRIPTION: Procedures and software to be embedded in application systems that allow for recording the contents of main memory at critical decision points within the application process. The intent of this safeguard is to allow the auditor an opportunity to examine logic paths during execution of the program.

PURPOSE: To detect unauthorized modification of programs.

APPLICABLE VULNERABILITY CATEGORIES: PMI, PME

COMMENTS: Retrofit

NAME: Audit from Terminal

CATEGORY: Audit 13

DESCRIPTION: Procedures and software to allow the ADP auditor to access, extract, manipulate, and display on-line data base information using a remote terminal. This type of safeguard is essentially the generalized audit software safeguard (Audit 11) for use in auditing on-line systems.

PURPOSE: To detect unauthorized modification of data.

APPLICABLE VULNERABILITY CATEGORIES: DMI, DME

COMMENTS: Retrofit

NAME: Library Usage Audit

CATEGORY: Audit 14

DESCRIPTION: Procedures and software to record and review the number of references to sensitive library modules by each application system or user and to verify the reasonableness of these entries. For example, if a user requests a specific tape more often than usual during a given time span, the auditor should verify that the requests were in accord with the user's work requirements.

PURPOSE: To detect unauthorized modification or disclosure of data or programs.

APPLICABLE VULNERABILITY CATEGORIES: DMI, DDiI, PMI, PDiI, DME, DDiE, PME, PDiE

COMMENTS: Retrofit

NAME: Late Processing Audit

CATEGORY: Audit 15

DESCRIPTION: Procedures and software to collect additional information on all jobs that are completed after their due dates and times. The intent of the audit is to ensure that control guidelines are not compromised as a consequence of the late processing.

PURPOSE: To detect unauthorized modification of data or programs.

APPLICABLE VULNERABILITY CATEGORIES: DMI, PMI, DME, PME

COMMENTS: Retrofit

NAME: Application System Design Verification

CATEGORY: Audit 16

DESCRIPTION: Procedures, software, and guidelines to ensure that ADP auditors verify the quantity and quality of internal controls specified by the user departments for inclusion in all new application systems. The verification should take place both before and after installation.

PURPOSE: To prevent all defined misuses.

APPLICABLE VULNERABILITY CATEGORIES: All

COMMENTS: Retrofit; This safeguard is the highest ranking prevention tool because it is believed that a very large number of misuses would have been prevented had organizations designed controls into the application system and taken steps to ensure that the controls were adequate and working before the system was declared operational.

NAME: Operations Area Surveillance

CATEGORY: Security 1

DESCRIPTION: Procedures and facilities to effect continuous surveillance of terminal and computer center at all times and of terminal areas during off-hours. Closed circuit TV (CCTV) can be used either manned or with video tape recording.

PURPOSE: To detect unauthorized modification, destruction, and disclosure (or theft) of data, programs, system equipment, or supplies.

APPLICABLE VULNERABILITY CATEGORIES: DME, DDeE, DDiE, PME, PDeE, PDiE, CE&SM, CE&SDe, CE&ST

COMMENTS: Retrofit; This safeguard was the highest ranking detection tool because of the large number of incidents in which an employee or perpetrator destroyed facilities, data or programs left in unmonitored areas.

NAME: Area Alarm System

CATEGORY: Security 2

DESCRIPTION: Software and facilities that provide for an alarm system to detect and record access to all critical areas, such as terminal room, supply room and computer center. Commercially available mini-computer-based systems provide an example.

PURPOSE: To detect unauthorized modification of data, programs, or system equipment; destruction of data, programs, system equipment, or supplies; and disclosure (or theft) of data, programs, system equipment, or supplies.

APPLICABLE VULNERABILITY CATEGORIES: DME, DDeE, DDiE, PME, PDeE, PDiE, CS&EM, CS&EDe, CS&ET

COMMENTS: Retrofit; Many cases exist in which perpetrators were allowed access to areas where they should not have been, but no one had the ability to detect their presence.

NAME: Data Center Access Control

CATEGORY: Security 3

DESCRIPTION: Procedures to restrict and control access to the data center including an authorized access list and a log for all entering and leaving the data center. Aspects of this safeguard may be automated using devices such as man-traps or badge readers.

PURPOSE: To prevent unauthorized modification, destruction, or theft of system equipment or supplies and denial of system service.

APPLICABLE VULNERABILITY CATEGORIES: CE&SM, CE&SDe, CE&ST, SSD

COMMENTS: Retrofit; In many cases, equipment was destroyed by demonstrators who were able to easily gain access to computer facilities or by persons who should not have been allowed in the center, even though they were employees of the company.

NAME: Fire Detection and Extinquishment

CATEGORY: Security 4

DESCRIPTION: Procedures and facilities to provide fire detection and extinquishment protection for all computer and user areas.

PURPOSE: To prevent destruction of data, programs, computer equipment, supplies and services.

APPLICABLE VULNERABILITY CATEGORIES: DDeE, PDeE, CE&SDe, SSD

COMMENTS: Retrofit is possible, albeit with some difficulty; A number of fire bombings during the late 1960's caused extensive fire damage to unprotected centers.

NAME: Internal Tampering Alarms

CATEGORY: Security 5

DESCRIPTION: Facilities to provide terminals and other remote devices with internal tampering alarms, including alarms against unplugging. This safeguard is an extension of safeguard Security 2, Area Alarm System.

PURPOSE: To prevent unauthorized modification or theft of terminals and other such equipment.

APPLICABLE VULNERABILITY CATEGORIES: CE&SM, CE&ST

COMMENTS: Difficult safeguard to apply without replacing terminals.

NAME: Metal Detector

CATEGORY: Security 6

DESCRIPTION: Procedures and facilities to provide for metal detection at the entrance to the computer center and remote computing facilities.

PURPOSE: To prevent destruction or theft of system equipment or supplies.

APPLICABLE VULNERABILITY CATEGORIES: CE&SDe, CE&ST

COMMENTS: Retrofit

NAME: X-Ray Surveillance

CATEGORY: Security 7

DESCRIPTION: Procedures and facilities to allow for X-ray of all packages, brief cases, tool boxes, and other such items leaving areas in which sensitive material is stored.

PURPOSE: To prevent disclosure of data or programs and theft of system equipment.

APPLICABLE VULNERABILITY CATEGORIES: DDiE, PDiE, CE&ST

COMMENTS: Retrofit

NAME: Package Control

CATEGORY: Security 8

DESCRIPTION: Procedures and facilities to provide for outgoing package control leaving areas in which sensitive material is stored, such as the tape and disk pack storage area. (This safeguard may be used in place of an X-ray machine.)

PURPOSE: To prevent unauthorized disclosure (or theft) of data, programs, computer equipment, or supplies.

APPLICABLE VULNERABILITY CATEGORIES: DDiE, PDiE, CE&ST

COMMENTS: Retrofit

NAME: Off-site Storage

CATEGORY: Security 9

DESCRIPTION: Procedures and facilities to effect secure off-site storage for copies of critical data files, programs, and documentation.

PURPOSE: To prevent denial of system service.

APPLICABLE VULNERABILITY CATEGORIES: SSD

COMMENTS: Retrofit

NAME: Computer Inventory Control

CATEGORY: Data Processing 1

DESCRIPTION: Procedures and software to effect inventory control of computer equipment, hardware replacement parts, unused media, and supplies, at all locations from arrival to end of useful life. The intent is to ensure a complete and consistent inventory control program that provides the auditor with sufficient information to verify the status of all inventory.

PURPOSE: To detect modification or theft of system equipment and supplies.

APPLICABLE VULNERABILITY CATEGORIES: CE&SM, CE&ST

COMMENTS: Retrofit

NAME: Bill Back System

CATEGORY: Data Processing 2

DESCRIPTION: Policy, procedures, and software to provide an accounting system for billing back all usage to the user organization. Costs should be broken out by department, project and person. To the extent possible, costs should be compared with budget projections.

PURPOSE: To detect unauthorized use of system services.

APPLICABLE VULNERABILITY CATEGORIES: SST

COMMENTS: Retrofit

NAME: Password Protection System

CATEGORY: Data Processing 3

DESCRIPTION: Policy, procedures, software, and facilities to provide a comprehensive password protection system to include compartmented initiation, disbursement, storage, and change of passwords. This information should be secured using safes, encryption, and other such means.

PURPOSE: To prevent unauthorized modification of data or programs; destruction (or disruption) of data, programs, or services; and disclosure (or theft) of data, programs, or services.

APPLICABLE VULNERABILITY CATEGORIES: DMI, DDeI, DDiI, PMI, PDeI, PDiI, SST, SSD

COMMENTS: Can be retrofit but with the degree of difficulty dependent on the organization size and usage of computers; While password systems were used in most organizations, they were used very poorly, i.e., passwords were never changed or were stored in clear text formats making it easy for a person to obtain the password.

NAME: Program Change Control Log

CATEGORY: Data Processing 4

DESCRIPTION: Procedures and software to effect complete control over program changes. Included are change logs and documentation as well as formal approval procedures.

PURPOSE: To prevent unauthorized modification of programs.

APPLICABLE VULNERABILITY CATEGORIES: PMI, PME

COMMENTS: Retrofit

NAME: Utility Control

CATEGORY: Data Processing 5

DESCRIPTION: Policy, procedures, and software to identify and control the use of specific system utilities that can bypass system integrity controls.

PURPOSE: To prevent unauthorized modification of data or programs and denial of system services.

APPLICABLE VULNERABILITY CATEGORIES: DMI, DDeI, DDiI, PMI, PDeI, PDiI, SSD

COMMENTS: Retrofit

NAME: Application System Test

CATEGORY: Application Interface 1
(Data Processing/System Control)

DESCRIPTION: Procedures, software, and guidelines to ensure thorough testing of application systems before operational status is acquired. Test items include internal controls, programming standard conventions, errors of omission and commission as well as recovery capability.

PURPOSE: To prevent application system failure.

APPLICABLE VULNERABILITY CATEGORIES: DMI, DDeI, DDiI, PMI, PDeI, PDiI, SSD, SST

COMMENTS: Retrofit; A number of misuses identified were a result of improperly tested systems. This was especially true in the university environment where students found ways to crash the system.

NAME: Program Standards

CATEGORY: Application Interface 2
(Data Processing/System Control)

DESCRIPTION: Procedures and software to ensure that all programs use accepted agency programming standards that might include items such as register conventions, standard parameter conventions and such.

PURPOSE: To prevent unauthorized modification or disclosure of data or programs.

APPLICABLE VULNERABILITY CATEGORIES: DMI, DDeI, DDiI, PMI, PDeI, PDiI, SST, SSD

COMMENTS: Retrofit

NAME: Test Isolation Control

CATEGORY: Application Interface 3
(Data Processing/System Control)

DESCRIPTION: Procedures, software, and hardware to isolate test systems from production systems, test data from live data, at all times. This isolation is accomplished by using hardware and software configuration controls.

PURPOSE: To prevent unauthorized modification or disclosure of data.

APPLICABLE VULNERABILITY CATEGORIES: DMI, DDiI

COMMENTS: Retrofit

NAME: Internal Standard Label Control

CATEGORY: Application Interface 4
(Data Processing/System Control)

DESCRIPTION: Procedures and software to ensure that application systems use standard labels for tapes, disks, and other removable media, to avoid bypassing system controls.

PURPOSE: To prevent unauthorized modification or disclosure of data or programs.

APPLICABLE VULNERABILITY CATEGORIES: DMI, DDiI, PMI, PDiI

COMMENTS: Retrofit

NAME: Documentation Control

CATEGORY: Application Interface 5
(Data Processing/System Control)

DESCRIPTION: Procedures, software, and facilities to control access to system and application documentation, stored in any format or medium.

PURPOSE: To prevent denial or theft of system service.

APPLICABLE VULNERABILITY CATEGORIES: SST, SSD

COMMENTS: Retrofit

NAME: User Command Log

CATEGORY: Internal Control 1
(Data Processing/System Control)

DESCRIPTION: Procedures and software to enable logging of user commands. The organization should establish application system standards that would require a selective logging capability for user commands.

PURPOSE: To detect unauthorized actions and monitor command activity by users.

APPLICABLE VULNERABILITY CATEGORIES: DMI, DDeI, DDiI, PMI, PDeI, PDiI, SSD , SST

COMMENTS: Retrofit; Users should be restricted to the fewest number of commands necessary to accomplish their task. In addition, application systems should have the capability to identify what commands were executed by each user at any time.

NAME: Data Transformation

CATEGORY: Internal Control 2
(Data Processing/System Control)

DESCRIPTION: Procedures and software that allow for storage of critical data elements in a slightly transformed format reversing the transformation before the data are used by application systems.

PURPOSE: To detect unauthorized disclosure of data.

APPLICABLE VULNERABILITY CATEGORIES: DDiI, DDiE

COMMENTS: Retrofit; This safeguard ranked so high because it worked very well against a few specific cases in a vulnerability category with few cases.

NAME: Sensitive File Access Log

CATEGORY: Internal Control 3
(Data Processing/System Control)

DESCRIPTION: Procedures and software to log all accesses, either by system programs or application programs, to files designated "sensitive" by the security administrator. The intent is to ensure an extra level of protection for "sensitive" files.

PURPOSE: To detect unauthorized accesses to sensitive files and generally monitor file access activity.

APPLICABLE VULNERABILITY CATEGORIES: DMI, DDeI, DDiI, PMI, PDeI, PDiI, SSD, SST

COMMENTS: Retrofit; In many of the cases reviewed, "sensitive" files were protected in the same manner as "nonsensitive" files.

NAME: Operator Console Log

CATEGORY: Internal Control 4
(Data Processing/System Control)

DESCRIPTION: Procedures and software to log specified commands issued at the operator console. For example, all privileged commands that allow modification of programs and/or data in main memory should be monitored.

PURPOSE: To detect unauthorized actions and to monitor command activity at the operator console.

APPLICABLE VULNERABILITY CATEGORIES: DMI, DDeI, DDiI, PMI, PDeI, PDiI, SSD, SST

COMMENTS: Retrofit

NAME: IPL Check

CATEGORY: Internal Control 5
(Data Processing/System Control)

DESCRIPTION: Procedures and software for use at initial program load (IPL) time to compare current system libraries against verified baseline system. Checksum programs that perform a special algorithm on each module are an example.

PURPOSE: To detect unauthorized modification of programs.

APPLICABLE VULNERABILITY CATEGORIES: PMI, PME

COMMENTS: Retrofit

NAME: Improper Log-on Control

CATEGORY: Internal Control 6
(Data Processing/System Control)

DESCRIPTION: Procedures and software to detect repeated attempts to log-on. For example, after three or four unsuccessful log-on attempts, a message might be sent to the console operator or to the security administrator's console for appropriate action.

PURPOSE: To detect unauthorized modification of data or programs; destruction (or disruption) of data, programs, or services; and disclosure (or theft) of data, programs, or services.

APPLICABLE VULNERABILITY CATEGORIES: DMI, DDeI, DDiI, PMI, PDeI, PDiI, SST, SSD

COMMENTS: Retrofit

NAME: Nonpassword Terminal User Verification

CATEGORY: Internal Control 7
(Data Processing/System Control)

DESCRIPTION: Procedures, software, and hardware to effect positive system verification of users at all terminals. Possible approaches include the use of ID cards and readers, handprint identifiers, or voice print identifiers.

PURPOSE: To prevent unauthorized modification, destruction, or disclosure of intellectual property or denial or theft of service or process.

APPLICABLE VULNERABILITY CATEGORIES: DMI, DDeI, DDiI, PMI, PDeI, PDiI, SST, SSD

COMMENTS: Difficult safeguard to apply without replacing or upgrading terminals.

NAME: Store and Fetch Protection

CATEGORY: Internal Control 8
(Data Processing/System Control)

DESCRIPTION: Software and hardware to effect store and fetch protection for both main and secondary storage. The intent of this safeguard is to confine the application system to its authorized storage areas.

PURPOSE: To prevent unauthorized modification or disclosure of data or programs; or theft or denial of service or process.

APPLICABLE VULNERABILITY CATEGORIES: DMI, DDeI, DDiI, PMI, PDeI, PDiI, SSD, SST

COMMENTS: Difficult to retrofit unless hardware capability is already present.

NAME: Least Privilege Principle

CATEGORY: Internal Control 9
(Data Processing/System Control)

DESCRIPTION: Procedures and software to check privileged commands to ensure that privilege requested is authorized for that individual or process. This check might be accomplished through use of a special system authorization table.

PURPOSE: To prevent unauthorized modification or disclosure of data or programs.

APPLICABLE VULNERABILITY CATEGORIES: DMI, DDiI, PMI, PDiI

COMMENTS: Retrofit

NAME: Privileged Use Controls

CATEGORY: Internal Control 10
(Data Processing/System Control)

DESCRIPTION: Procedures and software to ensure that a special password system exists for privileged users, such as operators or system programmers. For example, this system may allow for daily change of privileged use passwords.

PURPOSE: To prevent unauthorized modification of data or programs; destruction (or disruption) of data, programs, or services; and disclosure (or theft) of data, programs, or services.

APPLICABLE VULNERABILITY CATEGORIES: DMI, DDeI, DDiI, PMI, PDeI, PDiI, SST, SSD

COMMENTS: Retrofit

NAME: Secondary Storage Passwords

CATEGORY: Internal Control 11
(Data Processing/System Control)

DESCRIPTION: Procedures and software to enable password protection for programs and sensitive data maintained on secondary storage. The intent of this safeguard is to add a second level of password protection.

PURPOSE: To prevent unauthorized modification, destruction, or disclosure of data or programs.

APPLICABLE VULNERABILITY CATEGORIES: DMI, DDeI, DDiI, PMI, PDeI, PDiI

COMMENTS: Retrofit

NAME: Device ID

CATEGORY: Internal Control 12
(Data Processing/System Control)

DESCRIPTION: Software and hardware to make serial number ID of various equipment components accessible to programs. This is of special utility in providing positive identification of terminals and devices interacting with an application system.

PURPOSE: To prevent unauthorized modification or disclosure of data or programs.

APPLICABLE VULNERABILITY CATEGORIES: DMI, DDiI, PMI, PDiI

COMMENTS: Difficult to retrofit unless hardware capability is already present.

NAME: Off-hour Terminal Disconnect

CATEGORY: Internal Control 13
(Data Processing/System Control)

DESCRIPTION: Procedures or software to disconnect unneeded communication lines from system during off hours.

PURPOSE: To prevent unauthorized modification, destruction, or disclosure of intellectual property or denial or theft of service or process.

APPLICABLE VULNERABILITY CATEGORIES: DMI, DDeI, DDiI, PMI, PDeI, PDiI, SST, SSD

COMMENTS: Retrofit

NAME: Password Generation

CATEGORY: Internal Control 14
(Data Processing/System Control)

DESCRIPTION: Procedures and software to ensure generation of passwords that are difficult to guess or determine programatically.

PURPOSE: To prevent unauthorized modification of data or programs; destruction (or disruption) of data, programs, or services; and disclosure (or theft) of data, programs, or services.

APPLICABLE VULNERABILITY CATEGORIES: DMI, DDeI, DDiI, PMI, PDeI, PDiI, SST, SSD

COMMENTS: Retrofit

NAME: Password Print Suppress

CATEGORY: Internal Control 15
(Data Processing/System Control)

DESCRIPTION: Procedures, software, and hardware to inhibit the display of passwords entered at a terminal by the user. In some cases, an underprint facility may be satisfactory.

PURPOSE: To prevent unauthorized modification, destruction, or disclosure of intellectual property or denial or theft of service or process.

APPLICABLE VULNERABILITY CATEGORIES: DMI, DDeI, DDiI, PMI, PDeI, PDiI, SST, SSD

COMMENTS: Retrofit

NAME: System Masquerade Control

CATEGORY: Internal Control 16
(Data Processing/System Control)

DESCRIPTION: Software and hardware to prevent a user from issuing system-like prompts to a terminal. The intent is to ensure that users are not able to obtain sensitive identification information from other users by masquerading as the system.

PURPOSE: To prevent unauthorized modification, destruction, or disclosure of intellectual property or denial or theft of service or process.

APPLICABLE VULNERABILITY CATEGORIES: DMI, DDeI, DDiI, PMI, PDeI, PDiI, SST, SSD

COMMENTS: Retrofit

NAME: Simultaneous Access Control

CATEGORY: Internal Control 17
(Data Processing/System Control)

DESCRIPTION: Software and hardware to prevent simultaneous access to data in modes that would allow unauthorized modification. For example, a file should be lockable from the time a record is modified until appropriate control entries have been made in the master file and history file.

PURPOSE: To prevent unauthorized data modification.

APPLICABLE VULNERABILITY CATEGORIES: DMI

COMMENTS: Difficult to retrofit unless hardware capability is already present.

NAME: Storage Purge

CATEGORY: Internal Control 18
(Data Processing/System Control)

DESCRIPTION: Procedures, software, and hardware to overwrite all types of storage after use for sensitive processing. The intent is to discourage scavenging through residue information on magnetic medium.

PURPOSE: To prevent unauthorized disclosure of data or programs.

APPLICABLE VULNERABILITY CATEGORIES: DDiI, PDiI

COMMENTS: Retrofit

NAME: Processing Time Control

CATEGORY: Internal Control 19
(Data Processing/System Control)

DESCRIPTION: Procedures and software to check actual time of use against authorized time for the application. The intent is to restrict application systems to certain times of the day, month, or year for which it is authorized.

PURPOSE: To prevent unauthorized use or denial of system service.

APPLICABLE VULNERABILITY CATEGORIES: SST, SSD

COMMENTS: Retrofit

NAME: Hardware Monitors

CATEGORY: Hardware Support 1
(Data Processing/System Control)

DESCRIPTION: Procedures, software, hardware, and facilities to monitor channel usage by application system or location over time and match actual usage with predicted or historical usage records.

PURPOSE: To detect theft of system services.

APPLICABLE VULNERABILITY CATEGORIES: SST

COMMENTS: Retrofit

NAME: Remote Encryption Capability

CATEGORY: Hardware Support 2
(Data Processing/System Control)

DESCRIPTION: Software, hardware, and/or facilities to provide encryption capability for storing and processing sensitive data at remote data processing facilities. This capability must be consistent with the encryption mechanisms in use at the central facility.

PURPOSE: To prevent unauthorized disclosure of data.

APPLICABLE VULNERABILITY CATEGORIES: DDiE

COMMENTS: Retrofit

NAME: Encryption for Transport

CATEGORY: Hardware Support 3
(Data Processing/System Control)

DESCRIPTION: Software and facilities to encrypt data that are to be transported by a third party outside the computer facility.

PURPOSE: To prevent unauthorized disclosure of data.

APPLICABLE VULNERABILITY CATEGORIES: DDiE

COMMENTS: Retrofit

NAME: Communication Encryption

CATEGORY: Hardware Support 4
(Data Processing/System Control)

DESCRIPTION: Software and hardware to provide encryption of information passing over communication lines. Of particular interest is transmission of data over low-speed lines between terminal and computer.

PURPOSE: To prevent unauthorized disclosure of data.

APPLICABLE VULNERABILITY CATEGORIES: DDiI

COMMENTS: Retrofit is possible, but difficult.

NAME: Alternate Communication Paths

CATEGORY: Hardware Support 5
(Data Processing/System Control)

DESCRIPTION: Hardware and facilities to ensure that alternative communication paths exist for critical on-line systems. For example, ensure duplicate paths exist between the computer facility and the telephone company central office.

PURPOSE: To prevent denial of system service.

APPLICABLE VULNERABILITY CATEGORIES: SSD

COMMENTS: Retrofit is possible but with difficulty and expense.

NAME: Media Usage Log

CATEGORY: Operations 1 (Data Processing)

DESCRIPTION: Procedures to log all movement and usage of removable, sensitive media, possibly using controlled external labels and times of the mount and dismount by job and user.

PURPOSE: To detect unauthorized modification or disclosure of data or programs or unauthorized use.

APPLICABLE VULNERABILITY CATEGORIES: DMI, DDeI, DDiI, PMI, PDeI, PDiI, SST

COMMENTS: Retrofit

NAME: I/O Data Control

CATEGORY: Operations 2 (Data Processing)
Data Handling 2 (Operations Division)

DESCRIPTION: Procedures to ensure that specific control points exist for data movement throughout the user area. The intent is to provide for traceability and accountability.

PURPOSE: To prevent unauthorized modification or disclosure of data or programs.

APPLICABLE VULNERABILITY CATEGORIES: DME, DDiE, PME, PDiE

COMMENTS: Retrofit; The most numerous incidents of misuse identified are in the data-handling areas outside the computer system. Each organization has to develop specific control points that are meaningful with the context of its environment.

NAME: I/O Data Storage

CATEGORY: Operations 3 (Data Processing)
Data Handling 3 (Operations Division)

DESCRIPTION: Procedures and facilities to provide lockable storage for sensitive data, programs, and reports. This safeguard is not directed at government, classified material.

PURPOSE: To prevent unauthorized modification, destruction, or disclosure of data or programs.

APPLICABLE VULNERABILITY CATEGORIES: DME, DDeE, DDiE, PME, PDeE, PDiE

COMMENTS: Retrofit; In a large number of cases, had safes or other lockable storage been used, not only would much of the data disclosure problem been solved, but also much of the data and program destruction problem would have been reduced.

NAME: Tape/Disk Movement Control

CATEGORY: Operations 4 (Data Processing)

DESCRIPTION: Procedures and software to ensure control of movement of removable media through the operations area. This includes a capability for traceability and accountability. This safeguard includes requirement for external labels on all media.

PURPOSE: To prevent unauthorized disclosure of data or programs.

APPLICABLE VULNERABILITY CATEGORIES: DDiE, PDiE

COMMENTS: Retrofit

NAME: External Sensitive Area Access Control

CATEGORY: Operations 5 (Data Processing)
Data Handling 5 (Operations Division)

DESCRIPTION: Procedures and facilities to deny or control unauthorized personnel access to sensitive user work areas. The intent of this safeguard is to ensure that a minimum number of people have access to user work areas where they might be able to change records that are in a format they understand.

PURPOSE: To prevent unauthorized modification, destruction, or disclosure of data or programs.

APPLICABLE VULNERABILITY CATEGORIES: DME, DDeE, DDiE, PME, PDeE, PDiE

COMMENTS: Retrofit

NAME: Sensitive Operator Input Control

CATEGORY: Operations 6 (Data Processing)

DESCRIPTION: Procedures and software to restrict and control sensitive inputs and adjustments that can be made at the operator console without special authorization. The intent of this safeguard is to ensure that systems are designed or modified so as to minimize operator involvement.

PURPOSE: To prevent modification and disclosure of data or programs.

APPLICABLE VULNERABILITY CATEGORIES: DMI, DDiI, PMI, PDiI

COMMENTS: Retrofit

NAME: File Backup Standard

CATEGORY: Operations 7 (Data Processing)

DESCRIPTION: Procedures and software to ensure backup of critical files. This safeguard includes the requirement of a backup schedule for all files and programs to prompt operations personnel when backups are required. It also includes provision for proper user notification and supervision.

PURPOSE: To prevent denial of system service.

APPLICABLE VULNERABILITY CATEGORIES: SSD

COMMENTS: Retrofit

NAME: Card Password Protection

CATEGORY: Operations 8 (Data Processing)

DESCRIPTION: Procedures to ensure protection of pass ord information in punched cards, e.g., in JCL decks. For example, the safeguard might call for users to place their own card decks in the card reader.

PURPOSE: To prevent unauthorized modification, destruction, or disclosure of intellectual property or denial or theft of service or process.

APPLICABLE VULNERABILITY CATEGORIES: DMI, DDeI, DDiI, PMI, PDeI, PDiI, SST, SSD

COMMENTS: Retrofit

NAME: Sensitive Forms Control

CATEGORY: Operations 9 (Data Processing)

DESCRIPTION: Procedures to ensure that sensitive forms, such as checks and certificates are properly controlled and secured. For example: Each set of serially-numbered forms should be maintained in such a manner that an audit can account for all forms used and remaining in storage.

PURPOSE: To prevent theft of forms.

APPLICABLE VULNERABILITY CATEGORIES: CE&ST

COMMENTS: Retrofit

NAME: Expiration Date Control

CATEGORY: Operations 10 (Data Processing)

DESCRIPTION: Procedures and software to ensure that expiration date mechanisms are used properly on all files in which such mechanisms are applicable. The intent of the safeguard is to ensure that expiration dates are maintained and changed only by authorized persons.

PURPOSE: To prevent data and program modification and denial of system service.

APPLICABLE VULNERABILITY CATEGORIES: DMI, PMI, SSD

COMMENTS: Retrofit

NAME: Console Configuration Control

CATEGORY: Operations 11 (Data Processing)

DESCRIPTION: Software and hardware to effect hardwiring of the addresses of privileged terminals, such as the system operator console. The intent of this safeguard is to ensure that the addresses of privileged terminals are not program-changeable.

PURPOSE: To prevent unauthorized modification, destruction, or disclosure of intellectual property or denial or theft of service or process.

APPLICABLE VULNERABILITY CATEGORIES: DMI, DDeI, DDiI, PMI, PDeI, PDiI, SST, SSD

COMMENTS: Retrofit

NAME:	Configuration Control
CATEGORY:	Operations 12 (Data Processing)
DESCRIPTION:	Procedures to prevent compromise of any files in the event of a system reconfiguration due to malfunctioning equipment or scheduled maintenance. The intent of the safeguard is to ensure that all system configurations, including emergency configurations, do not allow data or program compromise.
PURPOSE:	To prevent unauthorized modification or disclosure of data or programs.
APPLICABLE VULNERABILITY CATEGORIES:	DMI, DDiI, PMI, PDiI
COMMENTS:	Retrofit

VULNERABILITY CATEGORY ABBREVIATIONS

CE&SDe:	Unauthorized Destruction of Computer Equipment or Supplies
CE&SM:	Unauthorized Modification of Computer Equipment or Supplies
CE&ST:	Theft of Computer Equipment or Supplies
DDeE:	Unauthorized Destruction of Data External to the Computer System
DDeI:	Unauthorized Destruction of Data Internal to the Computer System
DDiE:	Unauthorized Disclosure of Data Stored External to the Computer System
DDiI:	Unauthorized Disclosure of Data Stored Internal to the Computer System
DME:	Unauthorized Modification of Data External to the Computer System
DMI:	Unauthorized Modification of Data Internal to the Computer System
PDeE:	Unauthorized Destruction of Programs External to the Computer System
PDeI:	Unauthorized Destruction of Programs Internal to the Computer System
PDiE:	Unauthorized Disclosure of Programs Stored External to the Computer System
PDiI:	Unauthorized Disclosure of Programs Stored Internal to the Computer System
PME:	Unauthorized Modification of Programs External to the Computer System
PMI:	Unauthorized Modification of Programs Internal to the Computer System
SSD:	Denial of Computer System Services
SST:	Unauthorized Use of Computer System Services

NBS-114A (REV. 7-73)

U.S. DEPT. OF COMM. BIBLIOGRAPHIC DATA SHEET	1. PUBLICATION OR REPORT NO. NBS SP 500-25	2. Gov't Accession No.	3. Recipient's Accession No.

4. TITLE AND SUBTITLE
An Analysis of Computer Security Safeguards for Detecting and Preventing Intentional Computer Misuse

5. Publication Date
January 1978

6. Performing Organization Code

7. AUTHOR(S) Brian Ruder and J.D. Madden
Editor(s) Robert P. Blanc

8. Performing Organ. Report No.

9. PERFORMING ORGANIZATION NAME AND ADDRESS
Stanford Research Institute
Menlo Park, California 942025

10. Project/Task/Work Unit No.

11. Contract/Grant No.

12. Sponsoring Organization Name and Complete Address (Street, City, State, ZIP)
National Bureau of Standards
Department of Commerce
Washington, D.C. 20234

13. Type of Report & Period Covered
Final

14. Sponsoring Agency Code

15. SUPPLEMENTARY NOTES
Library of Congress Catalog Card Number: 77-25368

16. ABSTRACT (*A 200-word or less factual summary of most significant information. If document includes a significant bibliography or literature survey, mention it here.*)

Stanford Research Institute (SRI) has an extensive file of actual computer misuse cases. The National Bureau of Standards asked SRI to use these cases as a foundation to develop ranked lists of computer safeguards that would have prevented or detected the recorded intentional misuses.

This report provides a working definition of intentional computer misuse, a construction of a vulnerability taxonomy of intentional computer misuse, a list of 88 computer safeguards, and a model for classifying the safeguards. In addition, there are lists ranking prevention and detection safeguards, with an explanation of the method of approach used to arrive at the lists.

This report should provide the computer security specialist with sufficient information to start or enhance a computer safeguard program.

17. KEY WORDS (*six to twelve entries; alphabetical order; capitalize only the first letter of the first key word unless a proper name; separated by semicolons*)
Computer crime; computer fraud; computer misuse; computer safeguards; computer security; computer security model; privacy.

18. AVAILABILITY
[X] Unlimited
[ ] For Official Distribution. Do Not Release to NTIS
[X] Order From Sup. of Doc., U.S. Government Printing Office Washington, D.C. 20402, SD Cat. No. C13.10:500-25
[ ] Order From National Technical Information Service (NTIS) Springfield, Virginia 22151

19. SECURITY CLASS (THIS REPORT)	21. NO. OF PAGES
UNCLASSIFIED	80
20. SECURITY CLASS (THIS PAGE)	22. Price $2.40
UNCLASSIFIED	

☆ U. S. GOVERNMENT PRINTING OFFICE :1977--261-238/416

USCOMM-DC 29042-P74

Waste Heat Management Guidebook

A typical plant can save about 20 percent of its fuel—just by installing waste heat recovery equipment. But with so much equipment on the market, how do you decide what's right for you?

Find the answers to your problems in the *Waste Heat Management Guidebook*, a new handbook from the Commerce Department's National Bureau of Standards and the Federal Energy Administration.

The *Waste Heat Management Guidebook* is designed to help you, the cost-conscious engineer or manager, learn how to capture and recycle heat that is normally lost to the environment during industrial and commercial processes.

The heart of the guidebook is 14 case studies of companies that have recently installed waste heat recovery systems and profited. One of these applications may be right for you, but even if it doesn't fit exactly, you'll find helpful approaches to solving many waste heat recovery problems.

In addition to case studies, the guidebook contains information on:

- sources and uses of waste heat
- determining waste heat requirements
- economics of waste heat recovery
- commercial options in waste heat recovery equipment
- instrumentation
- engineering data for waste heat recovery
- assistance for designing and installing waste heat systems

To order your copy of the *Waste Heat Management Guidebook*, send $2.75 per copy (check or money order) to Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402. A discount of 25 percent is given on orders of 100 copies or more mailed to one address.

The *Waste Heat Management Guidebook* is part of the EPIC industrial energy management program aimed at helping industry and commerce adjust to the increased cost and shortage of energy.

U.S. DEPARTMENT OF COMMERCE/National Bureau of Standards
FEDERAL ENERGY ADMINISTRATION/Energy Conservation and Environment

ANNOUNCEMENT OF NEW PUBLICATIONS ON COMPUTER SCIENCE & TECHNOLOGY

Superintendent of Documents,
Government Printing Office,
Washington, D. C. 20402

Dear Sir:

Please add my name to the announcement list of new publications to be issued in the series: National Bureau of Standards Special Publication 500-.

Name _____

Company _____

Address _____

City _____ State _____ Zip Code _____

(Notification key N-503)

NBS TECHNICAL PUBLICATIONS

PERIODICALS

JOURNAL OF RESEARCH—The Journal of Research of the National Bureau of Standards reports NBS research and development in those disciplines of the physical and engineering sciences in which the Bureau is active. These include physics, chemistry, engineering, mathematics, and computer sciences. Papers cover a broad range of subjects, with major emphasis on measurement methodology, and the basic technology underlying standardization. Also included from time to time are survey articles on topics closely related to the Bureau's technical and scientific programs. As a special service to subscribers each issue contains complete citations to all recent NBS publications in NBS and non-NBS media. Issued six times a year. Annual subscription: domestic $17.00; foreign $21.25. Single copy, $3.00 domestic; $3.75 foreign.

Note: The Journal was formerly published in two sections: Section A "Physics and Chemistry" and Section B "Mathematical Sciences."

DIMENSIONS/NBS

This monthly magazine is published to inform scientists, engineers, businessmen, industry, teachers, students, and consumers of the latest advances in science and technology, with primary emphasis on the work at NBS. The magazine highlights and reviews such issues as energy research, fire protection, building technology, metric conversion, pollution abatement, health and safety, and consumer product performance. In addition, it reports the results of Bureau programs in measurement standards and techniques, properties of matter and materials, engineering standards and services, instrumentation, and automatic data processing.

Annual subscription: Domestic, $12.50; Foreign $15.65.

NONPERIODICALS

Monographs—Major contributions to the technical literature on various subjects related to the Bureau's scientific and technical activities.

Handbooks—Recommended codes of engineering and industrial practice (including safety codes) developed in cooperation with interested industries, professional organizations, and regulatory bodies.

Special Publications—Include proceedings of conferences sponsored by NBS, NBS annual reports, and other special publications appropriate to this grouping such as wall charts, pocket cards, and bibliographies.

Applied Mathematics Series—Mathematical tables, manuals, and studies of special interest to physicists, engineers, chemists, biologists, mathematicians, computer programmers, and others engaged in scientific and technical work.

National Standard Reference Data Series—Provides quantitative data on the physical and chemical properties of materials, compiled from the world's literature and critically evaluated. Developed under a world-wide program coordinated by NBS. Program under authority of National Standard Data Act (Public Law 90-396).

NOTE: At present the principal publication outlet for these data is the Journal of Physical and Chemical Reference Data (JPCRD) published quarterly for NBS by the American Chemical Society (ACS) and the American Institute of Physics (AIP). Subscriptions, reprints, and supplements available from ACS, 1155 Sixteenth St. N.W., Wash., D.C. 20056.

Building Science Series—Disseminates technical information developed at the Bureau on building materials, components, systems, and whole structures. The series presents research results, test methods, and performance criteria related to the structural and environmental functions and the durability and safety characteristics of building elements and systems.

Technical Notes—Studies or reports which are complete in themselves but restrictive in their treatment of a subject. Analogous to monographs but not so comprehensive in scope or definitive in treatment of the subject area. Often serve as a vehicle for final reports of work performed at NBS under the sponsorship of other government agencies.

Voluntary Product Standards—Developed under procedures published by the Department of Commerce in Part 10, Title 15, of the Code of Federal Regulations. The purpose of the standards is to establish nationally recognized requirements for products, and to provide all concerned interests with a basis for common understanding of the characteristics of the products. NBS administers this program as a supplement to the activities of the private sector standardizing organizations.

Consumer Information Series—Practical information, based on NBS research and experience, covering areas of interest to the consumer. Easily understandable language and illustrations provide useful background knowledge for shopping in today's technological marketplace.

Order **above** *NBS publications from: Superintendent of Documents, Government Printing Office, Washington, D.C. 20402.*

Order **following** *NBS publications—NBSIR's and FIPS from the National Technical Information Services, Springfield, Va. 22161.*

Federal Information Processing Standards Publications (FIPS PUB)—Publications in this series collectively constitute the Federal Information Processing Standards Register. Register serves as the official source of information in the Federal Government regarding standards issued by NBS pursuant to the Federal Property and Administrative Services Act of 1949 as amended, Public Law 89-306 (79 Stat. 1127), and as implemented by Executive Order 11717 (38 FR 12315, dated May 11, 1973) and Part 6 of Title 15 CFR (Code of Federal Regulations).

NBS Interagency Reports (NBSIR)—A special series of interim or final reports on work performed by NBS for outside sponsors (both government and non-government). In general, initial distribution is handled by the sponsor; public distribution is by the National Technical Information Services (Springfield, Va. 22161) in paper copy or microfiche form.

BIBLIOGRAPHIC SUBSCRIPTION SERVICES

The following current-awareness and literature-survey bibliographies are issued periodically by the Bureau:

Cryogenic Data Center Current Awareness Service. A literature survey issued biweekly. Annual subscription: Domestic, $25.00; Foreign, $30.00.

Liquified Natural Gas. A literature survey issued quarterly. Annual subscription: $20.00.

Superconducting Devices and Materials. A literature survey issued quarterly. Annual subscription: $30.00. Send subscription orders and remittances for the preceding bibliographic services to National Bureau of Standards, Cryogenic Data Center (275.02) Boulder, Colorado 80302.

U.S. DEPARTMENT OF COMMERCE
National Bureau of Standards
Washington, D.C. 20234

OFFICIAL BUSINESS

Penalty for Private Use, $300

POSTAGE AND FEES PAID
U.S. DEPARTMENT OF COMMERCE
COM-215

SPECIAL FOURTH-CLASS RATE
BOOK